Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Sesión 3. Cifrado Simétrico.

---

1. Describe el proceso de cifrado y descifrado asociado a un cifrador en bloque F usado en modo CTR. Supongamos se envía un mensaje de 5 bloques, y que al transmitir el bloque 3 de texto cifrado c_3 se produce un error (y al receptor le llega, en lugar de c_3, otra cosa $\hat{c}_3$. ¿Cuáles de los 5 bloques podrán ser descifrados correctamente por un receptor legítimo?

2. Redes de Feistel: responde a las siguientes preguntas.

   a) Explica la estructura de una red de Feistel y qué herramientas se diseñan típicamente a partir de ellas.

   b) Considera una red de Feistel extructurada en 3 rondas. Actuamos sobre bloques de 16 bits con una clave $K = k_1\| \cdots \|k_8$ formada por 8 bits, donde todas las funciones de ronda f_j son iguales y se definen como

   $$f_j(K, x) = x_1 \oplus k_1 \| x_2 \| x_3 \| x_4 \| x_5 \oplus k_2 \| x_6 \oplus k_7 \| x_7 \| x_8 \oplus k_8.$$

   Cifra el texto claro 0101000011110111. Comenta los fallos de diseño que te parezcan relevantes en la construcción anterior.

3. Verdadero o Falso (razona tu respuesta)

   a. La función l de expansión de un generador pseudoaleatorio cumple $l(n) < n$ para todo número natural n .

   b. El modo de operación OFB define el cifrado del bloque i-ésimo como

   $$c_i := m_i \oplus r_i,$$

   siendo m_i el i-ésimo bloque de texto claro y r_i un máscara que se calcula a partir de F, el cifrador en bloque utilizado.

   c. El cifrado AES se considera seguro a medio plazo (*legacy*) pero no a largo plazo (*future*).

   d. Toda función hash resistente a colisiones (CR) cumple la propiedad PR.